9

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-096121
(43)Date of publication of application : 09.04.1999

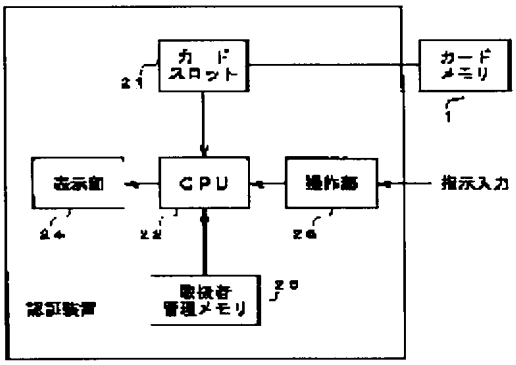
(51)Int.Cl. G06F 15/00

(21)Application number : 09-253960
(22)Date of filing : 18.09.1997

(71)Applicant : KOKUSAI ELECTRIC CO LTD
(72)Inventor : KAYANUMA TAKAAKI
TAKAZAWA HIDEAKI
TAKECHI EIJI

(54) CERTIFICATION DEVICE AND CERTIFICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a certification device and a certification system capable of preventing a card memory from being illegally used even when it is copied.
SOLUTION: When a CPU 22 attains certification, the certification device changes a certification code stored in a card memory 1 inserted into a card slot 21 and a handier management memory 23 and completing its certification. When the CPU 22 attains certification, the device changes a certification code stored in the card memory 1 inserted into the card slot 21 and a handler management memory 33 on a server and completing its certification.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－96121

(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

(21)出願番号　特願平9－253960

(22)出願日　平成９年(1997)９月18日

(71)出願人　000001122
国際電気株式会社
東京都中野区東中野三丁目14番20号

(72)発明者　董沼　隆昭
東京都中野区東中野三丁目14番20号　国際電気株式会社内

(72)発明者　高沢　秀明
東京都中野区東中野三丁目14番20号　国際電気株式会社内

(72)発明者　武地　永次
東京都中野区東中野三丁目14番20号　国際電気株式会社内

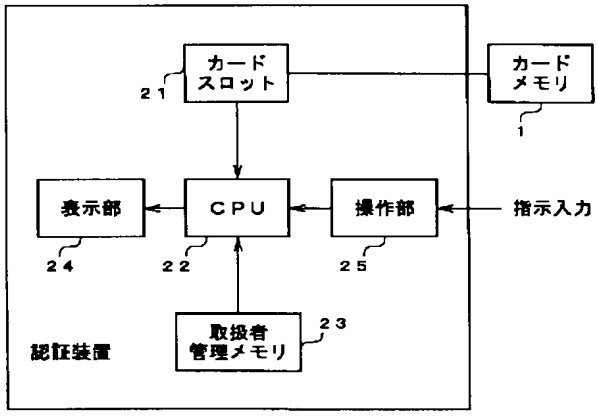
(74)代理人　弁理士　船津　暢宏　（外１名）

(54)【発明の名称】　認証装置及び認証システム

(57)【要約】

【課題】　従来の認証装置及び認証システムでは、カードメモリがコピーされると不正使用される虞があったが、本発明では、カードメモリがコピーされても不正使用を防止できる認証装置及び認証システムを提供する。

【解決手段】　ＣＰＵ２２が認証を達成したときに、カードスロット２１に挿入されているカードメモリ１と取扱者管理メモリ２３とに格納されている、認証が為された認証コードを変更する認証装置及び、ＣＰＵ２２が認証を達成したときに、カードスロット２１に挿入されているカードメモリ１とサーバ３上の取扱者管理メモリ３３とに格納されている、認証が為された認証コードを変更する認証システムである。



【特許請求の範囲】
【請求項１】　認証が為される毎に認証コードを変更することを特徴とする認証装置。
【請求項２】　メモリカードのインターフェイスであるカードスロットと、認証コードを格納する取扱者管理メモリとを具備し、認証が為されると、前記取扱者管理メモリに格納されている認証が為された認証コードを特定のコードで上書きして変更し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更することを特徴とする認証装置。
【請求項３】　メモリカードのインターフェイスであるカードスロットを具備する認証装置と、認証コードを格納する取扱者管理メモリを具備するサーバとを備え、
前記認証装置で認証が為されると、前記認証装置が特定のコードとともに前記サーバに前記取扱者管理メモリに格納されている認証が為された認証コードを当該特定のコードで上書きして変更する要求を送信出力し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更し、
前記サーバが、受信した前記要求にしたがって、前記取扱者管理メモリに格納されている前記認証コードを前記特定のコードで上書きして変更することを特徴とする認証システム。
【請求項４】　認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴とする請求項２記載の認証装置。
【請求項５】　認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴とする請求項３記載の認証システム。
【請求項６】　特定のコードは、認証が為された時刻を表すコードであることを特徴とする請求項２又は請求項４記載の認証装置。
【請求項７】　特定のコードは、認証装置において認証が為された時刻を表すコードであることを特徴とする請求項３又は請求項５記載の認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード等のカードメモリを利用して装置取扱者の認証を行う認証装置及び認証システムに係り、特に不正使用の防止をより強化できる認証装置及び認証システムに関する。
【０００２】
【従来の技術】認証装置は、不正使用を防止しようとする装置に装着し、利用者の認証が為されるまでは、当該装置の操作を禁止する動作を行うものである。
【０００３】一般的な認証装置及び認証システムについて、図１と図２とを参照しつつ説明する。図１は、認証装置の一般的な構成ブロック図であり、図２は、認証システムの一般的な構成ブロック図である。
【０００４】図１に示す認証装置は、カードメモリ１を挿入され、当該カードメモリ１のインターフェースとして動作するカードスロット２１と、ＣＰＵ２２と、取扱者管理メモリ２３と、表示部２４と、操作部２５とから構成されている。
【０００５】また、図２に示す認証システムは、カードスロット２１と、ＣＰＵ２２と、表示部２４と、操作部２５と、送受信部２６と、サーバ３とから構成されている。さらに、サーバ３は、送受信部３１と、ＣＰＵ３２と、取扱者管理メモリ３３とから構成されている。尚、図２に示す認証システムでは、複数の認証装置がネットワーク等を介してサーバ３に接続されていても構わない。
【０００６】まず、図１に示す認証装置について、以下、各部を具体的に説明する。カードメモリ１は、ユーザ名と認証コードとを対応づけて格納しているものであり、具体的には、図４に示すような内容のテーブルを格納しているものである。図４は、カードメモリ１に格納されているテーブルの内容の一例を表す説明図である。
【０００７】ＣＰＵ２２は、操作部２５から装置を使用しようとする旨の指示の入力を受けて、取扱者管理メモリ２３と、カードスロット２１に差し込まれたカードメモリ１の内容と、操作部２５から入力される操作の内容とを参照して規定の条件が満たされれば、装置の使用を許可するものである。ＣＰＵ２２における具体的な処理は後述する。
【０００８】取扱者管理メモリ２３は、図５に示すような内容のテーブルを格納しているものである。図５は、取扱者管理メモリ２３の内容の一例を表す説明図である。
【０００９】ここで、ＣＰＵ２２における認証の処理について図６を参照しつつ説明する。図６は、ＣＰＵ２２における認証の処理を表すフローチャート図である。ＣＰＵ２２は、操作部２５から装置を使用しようとする旨の指示の入力を受けて、カードスロット２１にカードメモリ１が挿入されているか否かを調べる（Ｓ１）。
【００１０】そして、カードメモリ１が挿入されていなければ（Ｎｏならば）、表示部２４にカードが挿入されていない旨のメッセージを表示出力し（Ｓ２）、処理終了する。
【００１１】また、処理Ｓ１において、カードスロット２１にカードメモリ１が挿入されていれば（Ｙｅｓであれば）、該カードメモリ１からユーザ名と認証コードとを読み出し（Ｓ３）、取扱者管理メモリ２３から対応するユーザ名を検索し、それに対応するパスワードを読み出す（Ｓ４）。
【００１２】そして、ＣＰＵ２２は、パスワードを要求する旨のメッセージを表示部２４に表示出力し（Ｓ５）、利用者から操作部２５を介してパスワードの入力を受けて、それが処理Ｓ４にて取扱者管理メモリ２３から読み出したパスワードと一致するか否かを調べる（Ｓ

６）。

【００１３】ここで、パスワードが一致しないと（Ｎｏであると）、パスワードが異なる旨のメッセージを表示部２４に表示出力し（Ｓ７）、処理終了する。また、処理Ｓ６において、パスワードが一致すると（Ｙｅｓであると）、取扱者管理メモリ２３から処理Ｓ４と同様に先に検索されるユーザ名に対応する認証コードを読み出す（Ｓ８）。

【００１４】そして、ＣＰＵ２２は、処理Ｓ３にてカードメモリ１から読み出した認証コードと取扱者管理メモリ２３から読み出した認証コードとが一致するか否かを調べ（Ｓ９）、一致すれば（Ｙｅｓならば）、認証が達成され、装置の操作を許可し（Ｓ１０）、処理終了する。

【００１５】また、処理Ｓ９において、認証コードが一致しなければ（Ｎｏならば）、表示部２４に「カードメモリが違います」等のメッセージを表示出力して（Ｓ１１）、処理を終了する。

【００１６】次に、図１に示す認証装置の動作について説明する。尚、以下の説明では、取扱者管理メモリ２３には、図５に示すようなテーブルが格納されているものとする。すなわち、ユーザ名「ＴＫＡＹＡ」には、パスワードとして「１」と、認証コードとして「ＴＫ１」とが対応づけられているとする。

【００１７】装置の利用者は、認証装置のカードメモリ１をカードスロット２１に挿入し、ＣＰＵ２２に装置を使用しようとする旨の指示を入力する。

【００１８】すると、ＣＰＵ２２がカードスロット２１に挿入されているカードメモリ１からユーザ名と認証コードとを読み出す。ここでは、説明のために、ユーザ名は「ＴＫＡＹＡ」であり、対応する認証コードは「ＴＫ１」であるとする。

【００１９】そして、ＣＰＵ２２が取扱者管理メモリ２３からユーザ名「ＴＫＡＹＡ」を検索し、それに対応して取扱者管理メモリ２３に格納されているパスワード「１」を読み出す。

【００２０】そして、ＣＰＵ２２が表示部２４にパスワードの入力を要求するメッセージを表示出力する。ここで、利用者がＣＰＵ２２にパスワード「１」を入力すると、ＣＰＵ２２が取扱者管理メモリ２３に格納されているパスワード「１」と入力されたパスワード「１」とが一致するので、さらに、取扱者管理メモリ２３からユーザ名「ＴＫＡＹＡ」に対応する認証コード「ＴＫ１」を読み出す。

【００２１】そして、読み出した認証コード「ＴＫ１」と、カードメモリ１に格納されている認証コード「ＴＫ１」と一致するかを調べると、それらが一致しているので、装置の使用を許可する。そして、利用者は、装置を操作できるようになる。

【００２２】次に、図２に示す認証システムの各部を具体的に説明する。ここで、カードスロット２１と、表示部２４と、操作部２５とは、図１に示すものと同様のものであるので、説明を省略する。また、サーバ３における取扱者管理メモリ３３は、図１に示す取扱者管理メモリ２３と同様のものであるので、説明を省略する。

【００２３】ＣＰＵ２２は、図１に示すＣＰＵ２２と同様のものであるが、図６に示す処理Ｓ４に代わって、サーバ３に送受信部２６を介してカードメモリ１から読み出したユーザ名に対応するパスワードを要求し、当該パスワードを受信するようになっているところと、処理Ｓ８に代わって、サーバ３に送受信部２６を介してカードメモリ１から読み出したユーザ名に対応する認証コードを要求し、当該認証コードを受信するようになっているところとが異なっている。

【００２４】サーバ３のＣＰＵ３２は、送受信部３１を介して認証装置のＣＰＵ２２からパスワードの要求を受けて、取扱者管理メモリ３３からパスワードを検索して送信出力するものであり、また、送受信部３１を介して認証装置のＣＰＵ２２から認証コードの要求を受けて、取扱者管理メモリ３３から認証コードを検索して送信出力するものである。

【００２５】従って、図２に示す認証装置は、取扱者管理メモリ２３を検索する代わりに、当該検索の指示をサーバ３に送信出力する以外は、図１に示す認証装置と同様の動作をするものである。

【００２６】

【発明が解決しようとする課題】しかしながら、上記認証装置及び認証システムにおける従来の認証方法では、カードメモリがパスワードを知り得る者によって不正にコピーされると、装置が不正使用される虞があり、また、そのような不正使用により装置を操作した記録が残らないという問題点があった。

【００２７】本発明は上記実情に鑑みて為されたもので、より高度に不正使用を防止し、不正使用の記録を残すことができる認証装置及び認証システムを提供することを目的とする。

【００２８】

【課題を解決するための手段】上記従来例の問題点を解決するための請求項１記載の発明は、認証装置において、認証が為される毎に認証コードを変更することを特徴としており、以前使用した認証コードを用いては認証を行えず、不正使用を防止できる。

【００２９】上記従来例の問題点を解決するための請求項２記載の発明は、認証装置において、メモリカードのインターフェイスであるカードスロットと、認証コードを格納する取扱者管理メモリとを具備し、認証が為されると、前記取扱者管理メモリに格納されている認証コードを特定のコードで上書きして変更し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更することを特徴としており、

メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる。

【００３０】上記従来例の問題点を解決するための請求項３記載の発明は、認証システムにおいて、メモリカードのインターフェイスであるカードスロットを具備する認証装置と、認証コードを格納する取扱者管理メモリを具備するサーバとを備え、前記認証装置で認証が為されると、前記認証装置が特定のコードとともに前記サーバに前記取扱者管理メモリに格納されている認証が為された認証コードを当該特定のコードで上書きして変更する要求を送信出力し、前記カードスロットに挿入されたメモリカードの認証コードを前記特定のコードで上書きして変更し、前記サーバが、受信した前記要求にしたがって、前記取扱者管理メモリに格納されている前記認証コードを前記特定のコードで上書きして変更することを特徴としており、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる。

【００３１】上記従来例の問題点を解決するための請求項４記載の発明は、請求項２記載の認証装置において、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴としており、請求項２記載の効果に加えて、不正な利用者の継続的な装置の不正使用を防止できる。

【００３２】上記従来例の問題点を解決するための請求項５記載の発明は、請求項３記載の認証システムにおいて、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにすることを特徴としており、請求項３記載の効果に加えて、不正な利用者の継続的な装置の不正使用を防止できる。

【００３３】上記従来例の問題点を解決するための請求項６記載の発明は、請求項２又は請求項４記載の認証装置において、特定のコードは、認証が為された時刻を表すコードであることを特徴としており、請求項２又は請求項４記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる。

【００３４】上記従来例の問題点を解決するための請求項７記載の発明は、請求項３又は請求項５記載の認証装置において、特定のコードは、認証が為された時刻を表すコードであることを特徴としており、請求項３又は請求項５記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる。

【００３５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係る認証装置（本装置）及び認証システムは、装置の使用を許可する毎に認証コードを変更するもので、不正使用を防止するとともに、不正使用が為された場合には、その事実を後に知ることができるものである。

【００３６】本装置は、図１に示した一般的な認証装置と同様の構成を備えるものであるが、ＣＰＵ２２における処理が少々異なっている。そこで以下、ＣＰＵ２２における処理について説明する。

【００３７】本装置のＣＰＵ２２は、従来と同様に、図６に示す処理を行うものであるが、処理Ｓ９において、処理Ｓ３にてカードメモリ１から読み出した認証コードと取扱者管理メモリ２３から読み出した認証コードとが一致して（Ｙｅｓであり）、認証が達成され、装置の操作を許可する処理Ｓ１０を処理する直前に、特定の方法で認証コードを新たに生成し、取扱者管理メモリ２３とカードメモリ１とに当該新たに生成した認証コードを書き込む処理（以下、「認証コード更新処理」と称する）を行うものである。

【００３８】ここで、ＣＰＵ２２の認証コード更新処理について、図３を用いて具体的に説明する。図３は、本装置におけるＣＰＵ２２の認証コード更新処理を表すフローチャート図である。まず、ＣＰＵ２２は、認証コード更新処理を行うに当たって、メモリカード１がカードスロット２１に挿入されているか否かを調べる（Ｓ２１）。そして、メモリカード１がカードスロット２１に挿入されていなければ（Ｎｏならば）、表示部２４にメモリカードの挿入を要求するメッセージを表示出力し（Ｓ２２）、処理Ｓ２１に移行する。

【００３９】また、処理Ｓ２１において、メモリカード１がカードスロット２１に挿入されていれば（Ｙｅｓならば）、新たに認証コードを生成し（Ｓ２３）、当該新たに生成した認証コードをカードメモリ１の認証コードに上書きして格納する（Ｓ２４）。

【００４０】そして、ＣＰＵ２２は、処理Ｓ２３で生成した認証コードを、メモリカード１に格納されているユーザ名に対応して取扱者管理メモリ２３に格納されている認証コードに上書きして格納し（Ｓ２５）、処理終了する。

【００４１】尚、処理Ｓ２３において認証コードを生成する方法として、例えば時刻を用いる方法が考えられる。すなわち、ＣＰＵ２２が処理Ｓ２３を実行する時刻が１５時２３分１９秒であったとすれば、認証コードとして「１５２３１９」を用いることとすればよい。このようにすれば、前回不正使用があった時刻を取扱者管理メモリ２３の内容として記録することができる効果がある。

【００４２】次に本装置の動作について説明する。尚、正規のメモリカード１の内容をコピーした不正なメモリカード１′が不正な利用者によって生成されているとする。ここで、正規のメモリカード１と不正なメモリカード１′とは同様のメモリカードであるが、区別のために符号を違えている。

【００４３】正規の利用者が正規のメモリカード１を本装置に挿入し、従来と同様にパスワードを入力すると、前回装置を使用した際に書き込まれている認証コード、例えば「１２００００」が取扱者管理メモリ２３とメモリカード１とに格納されており、それらが一致するので、装置が操作できるようになる。

【００４４】また、このとき、新たに認証コードが生成され、当該認証コード、例えば「１５２３１９」が取扱者管理メモリ２３とメモリカード１とに格納される。やがて、不正利用者が不正なメモリカード１′を本装置に挿入し、パスワードを入力するが、当該不正なメモリカード１′には、メモリカード１を不正にコピーした際の認証コード、例えば「１２００００」が格納されており、取扱者管理メモリ２３には変更された認証コードである「１５２３１９」が格納されているため、両者が一致せず、不正な利用者は、装置を操作することができない。

【００４５】本装置によれば、メモリカードが不正にコピーされても、コピーされてから一度でも正規のメモリカードを認証装置に挿入し、装置を操作すれば、取扱者管理メモリと当該正規のメモリカードとに格納されている認証コードが変更されるので、不正にコピーされたメモリカードを用いて装置を操作することができなくなり、不正使用を防止できる効果がある。

【００４６】また、本装置によれば、不正にコピーされたメモリカードを利用して装置が操作されると、当該不正にコピーされたメモリカードと取扱者管理メモリとに格納されている認証コードが変更されるので、次に正規のメモリカードを挿入しても装置を使用することができなくなるため、不正使用があったことを知ることができ、不正使用を記録できる効果がある。

【００４７】本発明の実施の形態に係る認証システム（本システム）は、図２に示す認証システムと同様に、ＣＰＵ２２が図６の処理Ｓ４とＳ８との代わりに、サーバ３に対して特定のユーザ名に対するパスワードと認証コードとを要求して受信するようになっており、また、図３の処理Ｓ２５の代わりに、サーバ３に対して特定のユーザ名に対する認証コードを書き換える要求を送信出力するものである。

【００４８】この場合のサーバ３のＣＰＵ３２は、特定のユーザ名に対する認証コードを書き換える要求をユーザ名と、新たな認証コードとともに送受信部３１を介して受信して、当該新たな認証コードを当該ユーザ名に対応して取扱者管理メモリ３３に格納されている認証コードに上書きして格納するようにすればよい。

【００４９】さらに、本装置及び本システムは、利用者がメモリカード１を用いて認証を行ったが、本装置の取扱者管理メモリ２３又は本システムのサーバ３の取扱者管理メモリ３３に格納されている認証コードと、当該メモリカード１に格納されている認証コードとが一致せず、認証が為されないと、当該ユーザ名による装置の使用を今後停止するものであっても構わない。

【００５０】つまり、ＣＰＵ２２が図６に示す処理Ｓ９において、認証コードが一致しないと（Ｎｏであると）、処理Ｓ１１によりカードメモリ１が異なる旨のメッセージを表示出力するとともに、当該ユーザ名による装置の使用を今後停止する。

【００５１】当該ユーザ名による装置の使用を停止するためには、例えば、図３に示した処理Ｓ２３と同様に認証コードを生成して、処理Ｓ２５と同様に本装置の取扱者管理メモリ２３又は本システムのサーバ３の取扱者管理メモリ３３における当該ユーザ名に対応する認証コードのみを新しく生成された認証コードで上書きし、カードメモリ１には上書きしないようにすることが考えられる。

【００５２】このようにした本装置又は本システムによれば、メモリカード１から認証コードを不正にコピーした場合に、正規の利用者よりも先に、当該不正なメモリカード１を所持する不正な利用者が一度でも使えば、取扱者管理メモリにおける認証コードが変わり、次に正規のカードメモリ１を用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用をできなくして、正規の利用者も装置の使用ができなくなるが、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【００５３】

【発明の効果】請求項１記載の発明によれば、認証が為される毎に認証コードを変更する認証装置としているので、以前使用した認証コードを用いては認証を行えず、不正使用を防止できる効果がある。

【００５４】請求項２記載の発明によれば、認証が為されると、取扱管理者メモリの認証コードとカードスロットに挿入したメモリカードの認証コードを同じ認証コードに変更する認証装置としているので、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる効果がある。

【００５５】請求項３記載の発明によれば、認証が為されると、サーバ上の取扱管理者メモリの認証コードとカードスロットに挿入したメモリカードの認証コードを同じ認証コードに変更する認証システムとしているので、メモリカードから認証コードを不正にコピーした場合に、その後一度でも正規のメモリカードを用いて認証を行っていれば、不正にコピーした認証コードでは認証を行えず、不正使用を防止できる効果がある。

【００５６】請求項４記載の発明によれば、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにする請求項２記載の認証装置としているので、メモリカードから認証コードを不

正にコピーした場合に、正規の利用者よりも先に、不正な利用者が一度でも不正なカードを用いて装置を使用すれば、取扱者管理メモリにおける認証コードが変わることとなり、その後正規のカードメモリを用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用を停止して、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【００５７】請求項５記載の発明によれば、認証が為されないと、当該認証が為されなかったユーザ名による装置の使用を以後できないようにする請求項３記載の認証システムとしているので、メモリカードから認証コードを不正にコピーした場合に、正規の利用者よりも先に、不正な利用者が一度でも不正なカードを用いて装置を使用すれば、取扱者管理メモリにおける認証コードが変わることとなり、その後正規のカードメモリを用いて正規の利用者が認証を行おうとすると、認証コードが異なるため、当該ユーザ名による装置の使用を停止して、不正な利用者の継続的な装置の不正使用を防止できる効果がある。

【００５８】請求項６記載の発明によれば、特定コードを認証が為された時刻を表すコードとした請求項２又は請求項４記載の認証装置としているので、請求項２又は請求項４記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる効果がある。

【００５９】請求項７記載の発明によれば、特定コードを認証が為された時刻を表すコードとした請求項３又は請求項５記載の認証装置としているので、請求項３又は請求項５記載の効果に加えて、不正使用が何時頃為されたのかを知ることができる効果がある。

【図面の簡単な説明】

【図１】認証装置の構成ブロック図である。

【図２】認証システムの構成ブロック図である。

【図３】本装置におけるＣＰＵ２２の認証コード更新処理を表すフローチャート図である。

【図４】カードメモリ１に格納されているテーブルの内容の一例を表す説明図である。

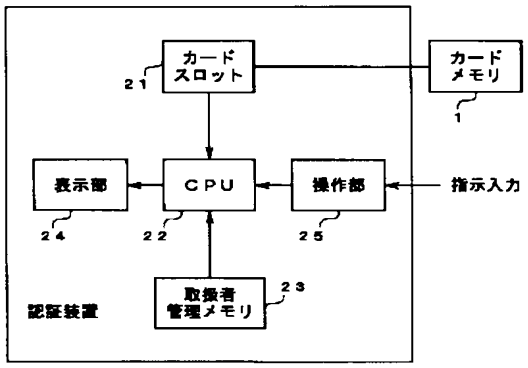
【図５】取扱者管理メモリ２３の内容の一例を表す説明図である。

【図６】ＣＰＵ２２における認証の処理を表すフローチャート図である。

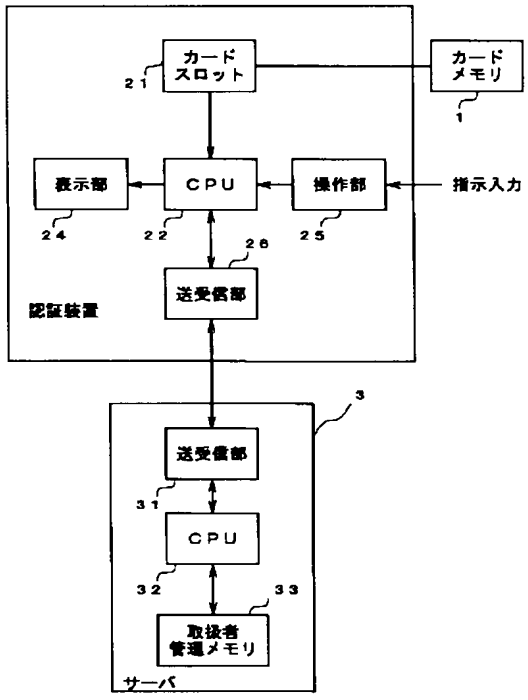
【符号の説明】

１…カードメモリ、　２１…カードスロット、　２２…ＣＰＵ、　２３…取扱者管理メモリ、　２４…表示部、　２５…操作部、　２６…送受信部、　３…サーバ、　３１…送受信部、　３２…ＣＰＵ、　３３…取扱者管理メモリ

【図１】



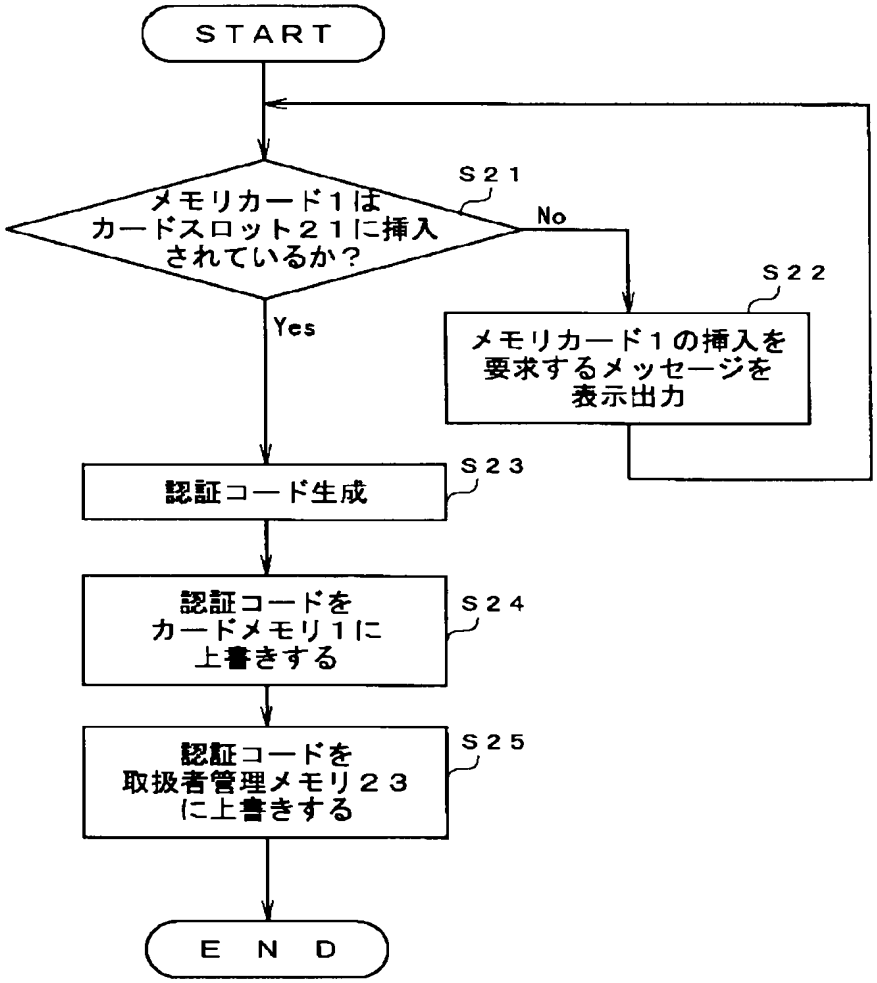
【図２】



【図４】

ユーザー名	認証コード
TKAYA	TK1

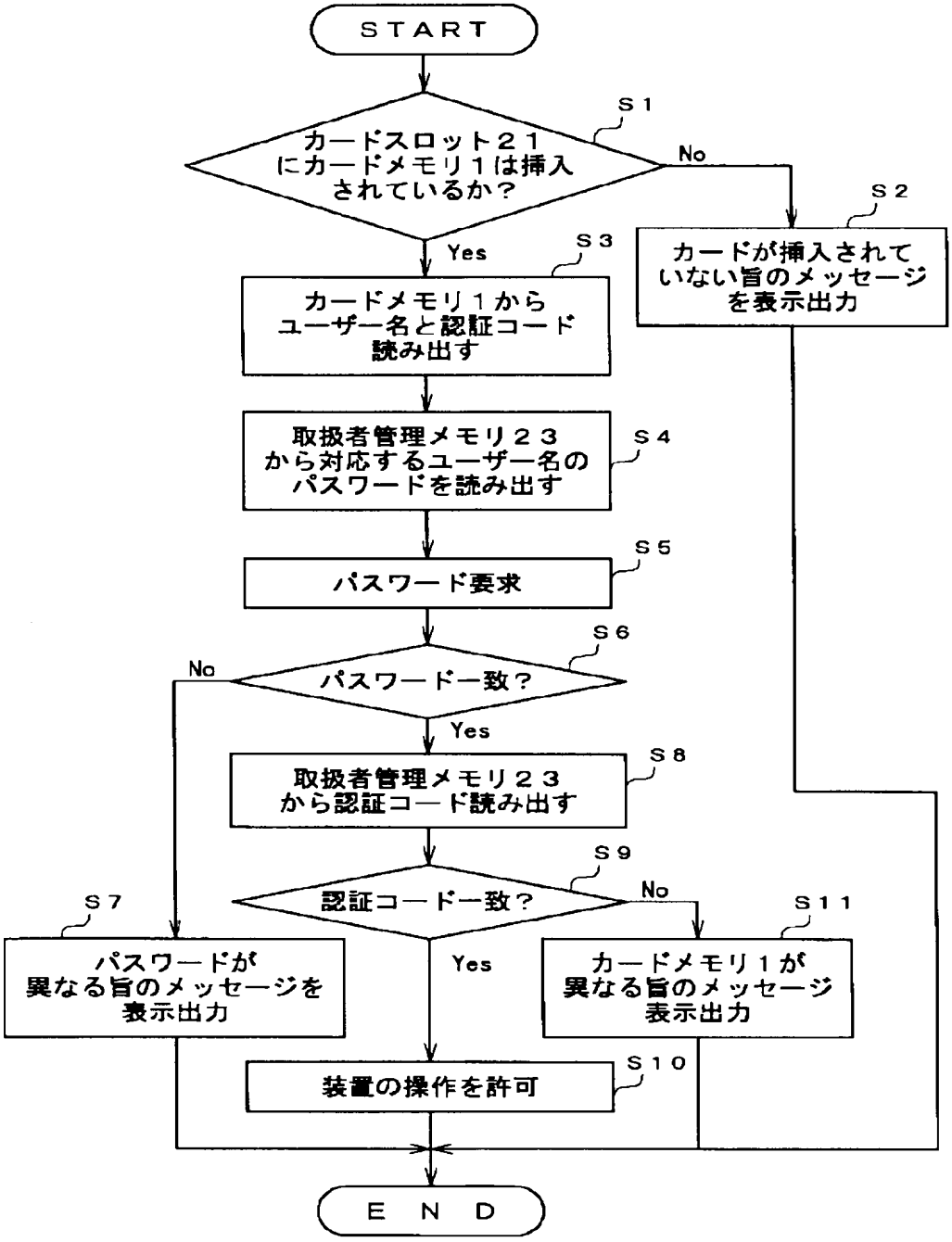
【図３】



【図５】

ユーザー名	パスワード	認証コード
TKAYA	1	TK1
ABC	XYZ	AABBCC
ICHIRO	16	7
⋮	⋮	⋮

【図６】


START
S１
カードスロット２１にカードメモリ１は挿入されているか？
No
S２
カードが挿入されていない旨のメッセージを表示出力
Yes
S３
カードメモリ１からユーザー名と認証コード読み出す
S４
取扱者管理メモリ２３から対応するユーザー名のパスワードを読み出す
S５
パスワード要求
S６
No
パスワード一致？
Yes
S８
取扱者管理メモリ２３から認証コード読み出す
S９
認証コード一致？
No
S１１
S７
パスワードが異なる旨のメッセージを表示出力
Yes
カードメモリ１が異なる旨のメッセージ表示出力
S１０
装置の操作を許可
E N D